IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
WUIDART

Serial No. **Not Yet Assigned**

Filing Date: **Herewith**

For: **SECURED MICROPROCESSOR COMPRISING A SYSTEM FOR ALLOCATING RIGHTS TO LIBRARIES**

I HEREBY CERTIFY THIS PAPER OR FEE IS BEING DEPOSITED WITH THE U.S. POSTAL SERVICE "EXPRESS MAIL POST OFFICE TO ADDRESSEE" SERVICE UNDER 37 CFR 1.10 ON THE DATE INDICATED BELOW AND IS ADDRESSED TO: BOX PATENT APPLICATIONS, ASSISTANT COMMISSIONER FOR PATENTS, WASHINGTON, D.C. 20231.

EXPRESS MAIL NO: EL747059127US

DATE OF DEPOSIT: June 20, 2001

NAME: Kyle Hopkinson

SIGNATURE:

09/885450 U.S. PTO 06/20/01

TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Director, U.S. Patent and Trademark Office
Washington, D.C. 20231

Sir:

Transmitted herewith is a certified copy of the priority French Application No. 0008283.

Respectfully submitted,

MICHAEL W. TAYLOR
Reg. No. 43,182
Allen, Dyer, Doppelt, Milbrath & Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
Telephone: 407/841-2330
Fax: 407/841-2343
Attorney for Applicant

R E P U B L I Q U E F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 30 AVR. 2001

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

CERTIFIED COPY OF PRIORITY DOCUMENT

INSTITUT NATIONAL DE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*01

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 W /260899

Réservé à l'INPI

REMISE DES PIÈCES
DATE 28 JUIN 2000
LIEU 13 INPI MARSEILLE
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0008283
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 28 JUIN 2000

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

OMNIPAT
MARCHAND André
24 Place des Martyrs de la Résistance
13100 AIX EN PROVENCE

Vos références pour ce dossier *(facultatif)* 100098 FR

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE	Cochez l'une des 4 cases suivantes
Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date / /
ou demande de certificat d'utilité initiale	N° Date / /
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date / /

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

MICROPROCESSEUR SECURISE COMPRENANT UN SYSTEME D'ATTRIBUTION DE DROITS A DES LIBRAIRIES

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE	
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	☐ S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»

5 DEMANDEUR		☐ S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»
Nom ou dénomination sociale		STMICROELECTRONICS
Prénoms		
Forme juridique		SOCIETE ANONYME
N° SIREN		3 4 1 4 5 9 3 8 6
Code APE-NAF		3 2 1 B
Adresse	Rue	7, Avenue Galliéni
	Code postal et ville	94250 GENTILLY CEDEX
Pays		FRANCE
Nationalité		FRANCE
N° de téléphone *(facultatif)*		
N° de télécopie *(facultatif)*		
Adresse électronique *(facultatif)*		

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE 2/2

Réservé à l'INPI

REMISE DES PIÈCES
DATE 28 JUIN 2000
LIEU 13 INPI MARSEILLE
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0008283

DB 540 W / 260899

Vos références pour ce dossier : *(facultatif)*		100098 FR
6 **MANDATAIRE**		
Nom		MARCHAND
Prénom		André
Cabinet ou Société		OMNIPAT
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	24 Place des Martyrs de la Résistance
	Code postal et ville	13100 AIX EN PROVENCE
N° de téléphone *(facultatif)*		04.42.99.06.60.
N° de télécopie *(facultatif)*		04.42.99.06.69.
Adresse électronique *(facultatif)*		
7 **INVENTEUR (S)**		
Les inventeurs sont les demandeurs		☐ Oui ☒ Non **Dans ce cas fournir une désignation d'inventeur(s) séparée**
8 **RAPPORT DE RECHERCHE**		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance		**Paiement en trois versements, uniquement pour les personnes physiques** ☐ Oui ☒ Non
9 **RÉDUCTION DU TAUX DES REDEVANCES**		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Requise antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence)* :
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

10 **SIGNATURE DU DEMANDEUR OU DU MANDATAIRE**
(Nom et qualité du signataire)
MARCHAND André - CPI N° 95 0303
OMNIPAT

VISA DE LA PRÉFECTURE OU DE L'INPI

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*02

DÉSIGNATION D'INVENTEUR(S) Page N° 1 / 1

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W /260899

Vos références pour ce dossier *(facultatif)* 13 INPI MARSEILLE	100098 FR
N° D'ENREGISTREMENT NATIONAL 0008283	

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

MICROPROCESSEUR SECURISE COMPRENANT UN SYSTEME D'ATTRIBUTION DE DROITS A DES LIBRAIRIES

LE(S) DEMANDEUR(S) :

MARCHAND André
OMNIPAT
24, Place des Martyrs de la Résistance
13100 AIX EN PROVENCE

DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).

Nom		WUIDART	
Prénoms		Sylvie	
Adresse	Rue	C/O OMNIPAT 24 Place des Martyrs de la Résistance	
	Code postal et ville	13100	AIX EN PROVENCE
Société d'appartenance *(facultatif)*			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance *(facultatif)*			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance *(facultatif)*			

DATE ET SIGNATURE(S)
DU (DES) DEMANDEUR(S)
OU DU MANDATAIRE
(Nom et qualité du signataire)

Aix en Provence, le 27 juin 2000
MARCHAND André - CPI N° 95 0303
OMNIPAT

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

MICROPROCESSEUR SECURISE COMPRENANT UN SYSTEME D'ATTRIBUTION DE DROITS A DES LIBRAIRIES

La présente invention concerne les microprocesseurs et plus particulièrement les microprocesseurs sécurisés.

Les microprocesseurs sécurisés sont fréquemment utilisés dans les applications où il est nécessaire d'interdire l'accès à certaines données ou programmes confidentiels. Ainsi, par exemple, les cartes à puce sont généralement équipées de microprocesseurs sécurisés afin de protéger les zones mémoire qui comprennent des codes confidentiels ou des algorithmes de cryptographie.

De façon classique, la sécurisation d'un microprocesseur est assurée par un système de contrôle d'adresses vérifiant que le programme en cours d'exécution est habilité à adresser certaines zones mémoire pour des opérations de lecture, d'écriture, de saut ou de branchement. Un tel système comprend généralement une table d'attribution de droits qui reçoit sur une première entrée un code d'identification du programme en cours d'exécution et sur une seconde entrée un code d'identification de la zone mémoire en cours d'adressage, correspondant à l'adresse courante présente sur le bus d'adresse du microprocesseur. S'il est prévu dans la table que la zone mémoire en cours d'adressage est accessible au programme en cours d'exécution, la table délivre un signal d'autorisation. Dans le cas contraire, la table ne délivre pas le signal d'autorisation et un signal de violation d'adresse est émis.

Un tel système de contrôle d'adresses permet de faire cohabiter de façon sécurisée divers programmes dans le plan mémoire d'un microprocesseur, en attribuant des droits différents à chacun des programmes. Ces divers programmes correspondent généralement à des applications

différentes du microprocesseur, prévues par le constructeur.

La sécurisation d'un microprocesseur a toutefois un effet négatif sur l'organisation du plan mémoire en ce qu'elle cloisonne le plan mémoire en diverses parties "étanches" les unes relativement aux autres, chaque partie étant réservée à une application. Or, il est fréquent que des programmes prévus pour des applications différentes comprennent des étapes de calcul similaires qui pourraient être centralisées dans une zone commune en tant que "librairie", une librairie désignant dans le langage de l'homme de l'art un ou plusieurs sous-programmes partagés par plusieurs programmes.

Cette méthode classique de centralisation sous forme de librairie de parties de programme communes à plusieurs programmes est généralement prohibée avec les microprocesseurs sécurisés en raison des problèmes de sécurité qu'elle entraîne. A titre d'exemple, supposons qu'un programme PGA bénéficie de droits pour accéder à une zone "X" du plan mémoire, et qu'un programme PGB bénéficie de droits pour accéder à une zone "Y" distincte de "X". La prévision d'un sous-programme partagé par les programmes PGA et PGB entraîne la question de savoir quels sont les droits qui doivent être conférés au sous-programme. Si le sous-programme doit pouvoir lire ou écrire des données dans la zone "X" lorsqu'il est appelé par le programme PGA et lire ou écrire dans la zone "Y" lorsqu'il est appelé par le programme PGB, il faut conférer au sous-programme les droits cumulés des programmes PGA et PGB, c'est-à-dire des droits sur la zone "X" et sur la zone "Y". Toutefois, le programme PGB ou un programme frauduleux chargé à l'emplacement du programme PGB pourrait utiliser le sous-programme pour accéder à la zone "X" réservée au programme PGA, et réciproquement. La prévision d'un sous-programme partagé par deux programmes ayant des droits d'accès différents

au plan mémoire constitue donc une brèche dans le cloisonnement du plan mémoire.

La présente invention vise à pallier cet inconvénient.

Plus particulièrement, la présente invention vise un moyen permettant de prévoir des sous-programmes partagés par plusieurs programmes sans porter atteinte à l'intégrité des droits conférés à chacun des programmes.

Cet objectif est atteint par la prévision d'un microprocesseur sécurisé comportant un système pour attribuer à des programmes exécutables par le microprocesseur des droits permanents d'accès à certaines zones du plan mémoire du microprocesseur, dans lequel le système d'attribution de droits comprend des moyens pour conférer à un sous-programme partagé par au moins deux programmes des droits temporaires d'accès à certaines zones mémoire lorsque le sous-programme est appelé par l'un des programmes, l'étendue des droits temporaires étant fonction du programme appelant le sous-programme.

Selon un mode de réalisation, le système d'attribution de droits comprend des moyens pour conférer temporairement à un sous-programme les droits du programme appelant.

Selon un mode de réalisation, le système d'attribution de droits comprend des moyens pour conférer en outre à un sous-programme des droits permanents indépendants de ceux du programme appelant.

Selon un mode de réalisation, le système d'attribution de droits comprend : une table d'attribution de droits agencée pour recevoir sur une première entrée un code d'identification d'un programme ou d'un sous-programme et sur une deuxième entrée un code d'identification des zones mémoire désignées par les adresses courantes circulant sur le bus d'adresse du microprocesseur ; et des moyens pour appliquer sur la première entrée de la table d'attribution de droits, pendant l'exécution d'un sous-programme, un code

d'identification du programme ayant appelé le sous-programme.

Selon un mode de réalisation, le système d'attribution de droits comprend des moyens pour appliquer simultanément sur la première entrée de la table d'attribution de droits, pendant l'exécution d'un sous-programme, un code d'identification du sous-programme en cours d'exécution et un code d'identification du programme ayant appelé le sous programme.

Selon un mode de réalisation, des bits du code d'identification du sous-programme en cours d'exécution et des bits du code d'identification du programme ayant appelé le sous programme sont combinés par une fonction logique avant d'être appliqués sur la première entrée de la table d'attribution de droits.

Selon un mode de réalisation, le système d'attribution de droits comprend : un premier verrou pour stocker pendant l'exécution d'une instruction le code d'identification du programme ou du sous-programme en cours d'exécution, et un second verrou ayant son entrée reliée à la sortie du premier verrou, agencé pour stocker le code d'identification d'un programme en cours d'exécution lorsque le microprocesseur bascule dans un sous-programme, pour former le code d'identification du programme ayant appelé le sous-programme, le second verrou étant remis à zéro lorsque le microprocesseur quitte le sous-programme.

Selon un mode de réalisation, le chargement et la remise à zéro du deuxième verrou sont contrôlés par un décodeur d'adresse recevant en entrée les adresses courantes circulant sur le bus d'adresse, agencé pour appliquer un signal de chargement au second verrou lorsque l'adresse de la première instruction d'un sous-programme est détectée, et délivrer au second verrou un signal de remise à zéro lorsque l'adresse de la dernière instruction du sous-programme est détectée.

Selon un mode de réalisation, les codes d'identification des zones mémoire désignées par les adresses courantes et les codes d'identification des programmes et sous-programmes en cours d'exécution sont délivrés par un décodeur d'adresse recevant en entrée les adresses courantes circulant sur le bus d'adresse.

Selon un mode de réalisation, le système d'attribution de droits émet un signal de violation quand une adresse présente sur le bus d'adresse ne correspond pas aux droits attribués de façon permanente ou temporaire au programme ou sous-programme en cours d'exécution.

Selon un mode de réalisation, le signal de violation d'adresse est traité par un décodeur d'interruption pour envoyer le microprocesseur dans un sous-programme de traitement des violations d'adresse.

Ces objets, caractéristiques et avantages ainsi que d'autres de la présente invention seront exposés plus en détail dans la description suivante d'un exemple de réalisation d'un microprocesseur selon l'invention, faite à titre non limitatif en relation avec les figures jointes parmi lesquelles :

- la figure 1 représente sous forme de bloc un microprocesseur comprenant un système de gestion de droits selon l'invention,
- la figure 2 représente le plan mémoire du microprocesseur et illustre un exemple d'application du système de gestion de droits selon l'invention,
- la figure 3 représente un exemple de réalisation d'une table d'attribution de droits en relation avec l'exemple illustré en figure 2, et
- les figures 4 et 5 représentent schématiquement deux autres exemples de réalisation d'une table d'attribution de droits selon l'invention.

La figure 1 représente sous forme de bloc un microprocesseur MP pourvu d'une mémoire morte MEM1 (ROM), d'une mémoire effaçable et programmable électriquement

MEM2 (EEPROM) et d'une mémoire vive MEM3 (RAM). Ces diverses mémoires sont reliées au microprocesseur par l'intermédiaire d'un bus d'adresse 1 et d'un bus de données 2, et forment ensemble le plan mémoire du microprocesseur.

Selon l'invention, le microprocesseur MP comprend un système d'attribution de droits 10 qui confère à des sous-programmes des droits d'accès variables en fonction du programme appelant.

Le système 10 comprend deux décodeurs d'adresse DEC1, DEC2 connectés en entrée au bus d'adresse pour recevoir les adresses courantes ADR circulant sur le bus d'adresse. Le décodeur DEC1 délivre un code CIM d'identification de zones mémoire du type :

$$CIM = b0\ b1...bn\ bn+1...bm$$

dans lequel chaque bit est affecté à l'identification d'une zone mémoire prédéterminée, un seul bit à la fois pouvant être à 1 pendant que les autres sont à 0.

Dans ce qui suit, on considérera que les bits b0 à bn sont affectés à la désignation de zones mémoire comprenant des programmes tandis que les bits bn+1 à bm sont affectés à la désignation de zones mémoire comprenant des données. Les zones programme sont par exemple localisées dans la mémoire MEM1 (ROM) tandis que les zones de données sont localisées dans les mémoires MEM2 et MEM3.

Les bits b0-bn du code CIM sont appliqués à l'entrée d'un verrou LT1 ("latch") piloté par un signal de chargement LOAD1 délivré par le microprocesseur MP. Lorsque le signal LOAD1 est appliqué au verrou LT1, la sortie du verrou recopie l'entrée du verrou et délivre un code CIP1 d'identification de zones programme.

Le code CIP1 est appliqué à l'entrée d'un second verrou LT2 piloté par un signal de chargement LOAD2 et un signal RST de remise à zéro délivrés par le décodeur

DEC2. Lorsque le signal LOAD2 est appliqué au verrou LT2, la sortie du verrou délivre un code CIP2 qui recopie le code CPI1 présent en entrée.

Les codes CIP1 et CIP2 sont combinés pour former un code résultant CIP3 qui est appliqué sur une entrée E1 d'une table d'attribution de droits TDA, recevant sur une entrée E2 le code CIM délivré par le décodeur DEC1. Dans le présent mode de réalisation, la combinaison des codes CIP1, CIP2 est assurée par une porte OU 11 dont la sortie délivre un code CIP3 égal à la somme logique bit à bit des codes CIP1 et CIP2.

La table d'attribution TDA comporte une sortie OUT constituée par des sorties élémentaires S_0-S_n, chaque sortie S_0-S_n correspondant à une entrée élémentaire de même rang $E1_1$... $E1_n$ de l'entrée E1, recevant l'un des bits du code CIP3. Les sorties S_0-S_n délivrent des droits d'accès sous forme de bits d'autorisation a_0 à a_n. Un bit d'autorisation a_i est égal à 1 lorsque l'entrée correspondante $E1_i$ reçoit un bit b_i égal à 1 et lorsque le code CIM appliqué sur l'entrée E2 comprend un bit b_j égal à 1 formant avec le bit b_i une combinaison autorisée $\{b_i, b_j\}$ de bits à 1. Les combinaisons autorisées $\{b_i, b_j\}$ sont enregistrées dans la table une fois pour toutes et définissent des droits permanents.

Le signal LOAD1 de chargement du verrou LT1 est délivré par le microprocesseur MP quand celui-ci lit ou est sur le point de lire une instruction dans la mémoire MEM1 (cycle de lecture ou cycle "fetch" du microprocesseur). A cet instant, l'adresse ADR présente sur le bus d'adresse est l'adresse IADR de l'instruction, délivrée par le compteur ordinal PC du microprocesseur. Ainsi, le code CIM délivré par le décodeur DEC1 comprend un bit b_i à 1 qui désigne la zone mémoire comprenant cette instruction. Ce bit b_i se retrouve dans le code CIP1 enregistré par le verrou LT1, et sur l'entrée E1 de la table TDA.

Par ailleurs, le signal LOAD2 est délivré par le décodeur DEC2 lorsque celui-ci détecte sur le bus 1 l'adresse ADRin de la première instruction d'un sous-programme partagé, et le signal RST est délivré par le décodeur DEC2 lorsque celui-ci détecte sur le bus d'adresse l'adresse ADRout de la dernière instruction du sous-programme. Les adresses ADRin, ADRout sont prédéterminées et représentent l'adresse d'entrée et l'adresse de sortie du sous-programme considéré. Si plusieurs sous-programmes sont partagés par des programmes, le décodeur DEC2 est agencé pour détecter les adresses d'entrée et de sortie de chacun des sous-programmes, et émettre le signal LOAD2 ou le signal RST quand l'une de ces adresses est détectée.

Le système 10 selon l'invention fonctionne de façon classique pendant l'exécution d'un programme, car la sortie du verrou LT2 est à 0, le code CIP3 appliqué à la table TDA étant ainsi égal au code CIP1. Pendant l'exécution du programme, après le chargement de chaque nouvelle instruction, il est fréquent que l'adresse courante ADR sur le bus d'adresse change et désigne une autre zone de la mémoire, par exemple lorsque l'instruction en cours d'exécution est une instruction de lecture ou d'écriture dans le plan mémoire. Dans ce cas, le code CIM délivré par le décodeur DEC1 change de valeur et présente un bit b_j à 1 différent, qui désigne la zone mémoire correspondante. Si la combinaison $\{b_i, b_j\}$ appliquée à la table TDA est autorisée, la sortie S_i de la table reste à 1. Sinon, la sortie S_i passe à 0 et le signal de violation VLT passe à 1. Après l'exécution de l'instruction, l'adresse IADR de la nouvelle instruction est émise sur le bus d'adresse et entraîne un autre changement du code CIM et la vérification automatique dans la table TDA d'une autre combinaison $\{b_i, b_j\}$ de bits de code. Si cette adresse correspond à un saut dans un sous-programme, une autorisation correspondante doit être prévue dans la table TDA.

Le fonctionnement du système 10 selon l'invention diffère d'un système de contrôle d'adresse classique lorsque le programme comprend une instruction de saut ou de branchement vers un sous-programme partagé. A l'instant où l'adresse ADRin de la première instruction du sous-programme se trouve sur le bus d'adresse, le décodeur DEC2 délivre le signal LOAD2 et le verrou LT2 enregistre le code CIP1 avant que le microprocesseur ne bascule dans le sous-programme. Ainsi, lorsque le microprocesseur a basculé dans le sous-programme, le code CIP1 à la sortie du verrou LT1 désigne la zone mémoire contenant le sous-programme tandis que le code CIP2 à la sortie du verrou LT2 désigne la zone mémoire dans laquelle se trouve le programme ayant appelé le sous-programme. Le code CIP1 identifie ainsi le sous-programme en cours d'exécution et le code CIP2 identifie le programme ayant appelé le sous-programme.

Les codes CIP1, CIP2 étant combinés ici dans la porte OU 11, la table TDA reçoit sur son entrée E1 un code CIP3 qui comprend deux bits b_i à 1 au lieu d'un seul, le premier correspondant au sous-programme en cours d'exécution et le second au programme ayant appelé le sous-programme. L'application à la table TDA du bit b_i correspondant au programme appelant autorise des combinaisons de bits $\{b_i, b_j\}$ avec les bits du code CIM qui sont spécifiques au programme appelant. Le sous-programme appelé "hérite" ainsi, pendant son exécution, des droits conférés au programme appelant. Ces droits transférés au sous-programme s'additionnent aux droits permanents qui lui sont attribués, ces droits pouvant toutefois être choisis nuls.

Le système 10 selon l'invention réalise ainsi une attribution dynamique de droits à un sous-programme appelé, qui cesse lorsque le microprocesseur retourne dans le programme appelant, au moment où le décodeur DEC2 détecte l'adresse de sortie ADRout du sous-programme et remet le code CIP2 à zéro.

En pratique, le signal VLT qui est émis lorsqu'une violation d'un droit permanent ou temporaire se produit, peut être utilisé de diverses manières pour empêcher l'accès à la zone mémoire interdite. Comme représenté en figure 1, le signal VLT est par exemple appliqué sur une entrée d'un décodeur d'interruption ITDEC dont la sortie délivre l'adresse ITADR d'un sous-programme de traitement des cas de violation d'adresse. L'adresse ITADR est appliquée sur une entrée d'un multiplexeur MUX qui reçoit sur une autre entrée l'adresse IADR de l'instruction suivante, délivrée par le compteur ordinal PC. Le multiplexeur est piloté par un signal IT délivré par le décodeur ITDEC et délivre au bus d'adresse l'adresse ITADR au lieu de l'adresse IADR lorsque le signal IT est émis. Dans une variante de réalisation, le signal VLT est utilisé pour forcer à 0 le signal de remise à zéro du microprocesseur (RESET), de manière à désactiver ce dernier. Dans une autre variante, le signal VLT est utilisé pour générer une interruption non masquable.

Le fonctionnement du système 10 selon l'invention sera mieux compris à la lumière d'un exemple simple de mise en œuvre qui est illustré en figure 2.

La figure 2 représente le plan mémoire du microprocesseur dans lequel certaines zones mémoire sont réservées à des applications, les autres étant strictement interdites et représentées hachurées. On distingue ainsi une zone A dans laquelle est enregistré un programme PGA, une zone B dans laquelle est enregistré un programme PGB, une zone C dans laquelle est enregistré un sous-programme LIB (librairie) partagé par les programmes PGA et PGB, une zone de données D réservée en écriture et en lecture au programme PGA, une zone de données E réservée en écriture et en lecture au programme PGB, une zone de données F réservée en écriture et en lecture au sous-programme LIB, et une zone G disponible en écriture et lecture aux trois programmes PGA, PGB, LIB. Les zones A, B, C sont par exemple agencées dans la

mémoire MEM1 (ROM), les zones D, E, F agencées dans la mémoire MEM2 (EEPROM) et la zone G dans la mémoire MEM3 (RAM). Comme représenté, le code CIM d'identification des zones mémoire comprend ainsi sept bits de code b0 à b6 affectés respectivement à l'identification des zones A à G, et les codes CIP1, CIP2 d'identification des zones programme comprennent les bits b0, b1 et b2.

Dans cet exemple, on souhaite que le sous-programme LIB bénéficie des droits du programme PGA ou PGB qui l'appelle, de manière que le programme PGA puisse demander au sous-programme d'enregistrer dans la zone D des résultats d'étapes de calcul et que le programme PGB puisse demander au sous-programme d'enregistrer dans la zone E de tels résultats, les zones F et G étant utilisables en tant que droits permanents par le sous-programme pour stocker des résultats temporaires.

Dans l'art antérieur, la solution pour atteindre cet objectif pourrait consister dans le fait d'attribuer au sous-programme des droits permanents sur les zones D et E, mais cela constituerait une brèche dans le cloisonnement du plan mémoire.

Selon l'invention, les droits sur l'une des zones D et E sont attribués temporairement au sous-programme en fonction du programme appelant, au moment où le microprocesseur entre dans le sous-programme.

Pour fixer les idées, la figure 3 représente un exemple de réalisation d'une table TDA1 permettant de générer une telle attribution de droits temporaires. La table TDA1 comprend trois lignes horizontales LH0 à LH2, sept lignes verticales LV0 à LV6 et trois lignes de sortie LS0 à LS2. Afin de faciliter la compréhension de ce qui suit, les bits du code CIP1 d'identification du programme en cours d'exécution sont référencés b0' à b2' et les bits du code CIP2 d'identification du programme appelant le sous-programme sont référencés b0" à b2".

Les lignes verticales LV0 à LV6 reçoivent respectivement les bits b0 à b6 du code CIM. La ligne LH0

reçoit le résultat de l'addition logique des bits b0' et b0". La ligne LH1 reçoit le résultat de l'addition logique des bits b1' et b1". La ligne LH2 reçoit le bit b2' seulement, car le bit b2" est toujours à 0. Les lignes LS0 à LS2 délivrent respectivement des bits d'autorisation a0 à a2 qui sont combinés dans la porte 12 pour former le signal VLT.

Les droits permanents d'accès au plan mémoire à attribuer aux programmes PGA, PGB et au sous-programme LIB sont matérialisés par des transistors MOS Ti,j agencés aux croisements des lignes horizontales LHi et des lignes verticales LVj. Un transistor Ti,j agencé au croisement de deux lignes LHi, LVj est connecté par sa grille à la ligne LHi, par son drain à la ligne LVj et par sa source à la ligne de sortie LSi. Ici, on distingue ainsi des transistors aux croisements de la ligne LH0 avec les lignes LV0, LV2, LV3 et LV6, qui déterminent les droits permanents du programme PGA sur sa propre zone mémoire A, sur la zone C contenant le sous-programme LIB et sur les zones D et G (fig. 2). On distingue également des transistors au croisement de la ligne LH1 avec les lignes LV1, LV2, LV4 et LV6, qui déterminent les droits permanents du programme PGB, et des transistors au croisement de la ligne LH2 et des lignes LV2, LV5 et LV6, qui déterminent les droits permanents du sous-programme LIB sur sa propre zone mémoire C et sur les zones F et G.

Le fonctionnement de la table TDA1 est en soi classique en ce qui concerne l'attribution des droits permanents aux programmes PGA, PGB, LIB. Chaque ligne de sortie LS0 à LS1 est maintenue à 0 par une résistance, respectivement r1 à r3, et est portée à 1 lorsqu'un transistor Ti,j connecté par sa source à la ligne de sortie reçoit un bit à 1 sur sa grille et sur son drain, le "1" logique correspondant à la tension d'alimentation du système.

L'attribution des droits temporaires et permanents du sous-programme intervient lorsque le microprocesseur

bascule dans le sous-programme. A cet instant, le bit b2' du code CIP1 est à 1, ce qui active les droits du sous-programme. De plus, le bit b0" ou le bit b1" du code CIP2 est également à 1 selon que le sous-programme a été appelée par le programme PGA ou PGB, ce qui maintient les droits du programme PGA ou PGB au bénéfice du sous-programme.

Bien entendu, la table TDA1 est en elle-même susceptible de diverses variantes de réalisation, notamment en logique inversée, qui sont à la portée de l'homme de l'art.

Par ailleurs, bien que l'on ait proposé dans ce qui précède de transférer à un sous-programme les droits du programme appelant, diverses autres variantes de la présente invention peuvent être prévues en ce qui concerne l'étendue des droits temporaires attribués à des sous-programmes.

A titre d'exemple, la figure 4 représente une table TDA2 ayant les mêmes lignes verticales LV0 à LV6 que la table TDA1 mais comprenant quatre lignes horizontales LH0 à LH3 recevant respectivement les bits b0', b1', b0" et b1" sans combinaison logique de ces bits. Les transistors Ti,j aux intersections des lignes sont représentés schématiquement par des points reliés par des flèches aux lignes de sortie, ici quatre lignes LS0 à LS3. Aucune ligne horizontale n'est prévue ici pour attribuer des droits permanents au sous-programme LIB, qui sont donc nuls dans cet exemple mais pourraient également être prévus non nuls.

La table TDA2 diffère de la table TDA1 en ce que les lignes LH0 et LH1 définissent les droits permanents des programmes PGA et PGB tandis que les lignes LH2, LH3, qui ne sont activées que par les bits b0" et b1", définissent les droits temporaires du sous-programme LIB. Les lignes LH2, LH3 étant distinctes et indépendantes des lignes LH0, LH1, il est possible d'attribuer au sous-programme, en fonction du programme appelant, des droits

temporaires distincts des droits permanents du programme appelant. Ainsi, dans l'exemple représenté, les transistors Ti,j sont agencés de manière que soient attribués :

- au programme PGA, des droits sur sa propre zone programme A, des droits sur la zone programme C du sous-programme LIB et des droits sur la zone G,
- au programme PGB, des droits sur sa propre zone programme B, des droits sur la zone programme C du sous-programme LIB et des droits sur la zone G,
- au sous-programme LIB, lorsqu'il est appelé par le programme PGA, des droits sur sa propre zone programme C et des droits sur les zones E et G,
- au sous-programme LIB, lorsqu'il est appelé par le programme PGB, des droits sur sa propre zone programme C et des droits sur les zones F et G,

En définitive, la prévision de deux lignes particulières LH2, LH3 recevant les bits b0", b1" enregistrés par le verrou LT2 au moment du basculement dans le sous-programme, permet d'attribuer au sous-programme des droits particuliers qui dépendent du programme appelant tout en étant indépendant des droits de ce dernier.

Par ailleurs, il apparaît dans cet exemple que les droits attribués au sous-programme LIB sont également attribués à tout autre sous-programme susceptible d'être appelé par les programmes PGA et PGB, puisque l'attribution de droits ne repose que sur les bits b0", b1" du code CIP2.

La figure 5 représente une table TDA3 qui est similaire à la table TDA2 mais dans laquelle la ligne LH2 reçoit le bit b0" combiné au bit b2' au moyen d'une porte ET, et la ligne LH3 reçoit le bit b1" combiné au bit b2' au moyen d'une autre porte ET. Dans ce cas, la ligne LH2 ou la ligne LH3 ne peut être activée qu'à la double condition que le bit b2' soit égal à 1 et que le bit b0" ou b1" soit également à 1. Ainsi, le transfert temporaire

de droits est réservé ici au sous-programme LIB à l'exclusion de tout autre sous-programme éventuel.

La présente invention est bien entendu susceptible de diverses autres variantes et modes de réalisation basés sur le principe selon l'invention d'un transfert de droits temporaires à des sous-programmes par mémorisation de l'identité du programme appelant. Notamment, des transferts de droits en cascades pourraient être prévus pour des sous-programmes de deuxième niveau appelés par des sous-programmes de premier niveau qui sont eux-mêmes appelés par des programmes principaux.

Enfin, bien que les modes de réalisation de tables d'attribution de droits qui sont décrits plus haut ont été présentés sous la forme de circuits matriciels à transistors, dans le souci de faciliter la compréhension de l'invention, il doit être noté qu'une table d'attribution de droits selon l'invention est susceptible en pratique de revêtir diverses autres formes. Notamment, une telle table est réalisable sous la forme d'un circuit à logique booléenne généré automatiquement par un compilateur de langage VHDL, cette méthode de génération automatique de circuits logiques à partir d'une fonction écrite en langage de haut niveau ayant connu un important essor ces dernières années.

REVENDICATIONS

1. Microprocesseur sécurisé (MP) comportant un système (10) pour attribuer à des programmes exécutables par le microprocesseur des droits permanents d'accès à certaines zones (A-G) du plan mémoire (MEM1-MEM3) du microprocesseur, caractérisé en ce que le système d'attribution de droits (10) comprend des moyens (DEC2, LT2) pour conférer à un sous-programme (LIB) partagé par au moins deux programmes (PGA, PGB) des droits temporaires d'accès à certaines zones mémoire lorsque le sous-programme est appelé par l'un desdits programmes, l'étendue des droits temporaires étant fonction du programme appelant le sous-programme.

2. Microprocesseur selon la revendication 1, caractérisé en ce que le système d'attribution de droits (10) comprend des moyens (TDA, TDA1, 11) pour conférer temporairement à un sous-programme (LIB) les droits du programme appelant (PGA, PGB).

3. Microprocesseur selon l'une des revendications 1 et 2, caractérisé en ce que le système d'attribution de droits comprend des moyens (TDA, TDA1, 11) pour conférer en outre à un sous-programme des droits permanents (F, G) indépendants de ceux du programme appelant.

4. Microprocesseur selon l'une des revendications 1 à 3, caractérisé en ce que le système d'attribution de droits comprend :

- une table (TDA, TDA1, TAD2, TDA3) d'attribution de droits agencée pour recevoir sur une première entrée (E1) un code (CIP1, b0-bn) d'identification d'un programme ou d'un sous-programme et sur une deuxième entrée (E2) un code (CIM, b0-bm) d'identification des zones mémoire désignées par les adresses courantes (ADR) circulant sur le bus d'adresse du microprocesseur, et

- des moyens (DEC2, LT2) pour appliquer sur la première entrée (E1) de la table d'attribution de droits, pendant l'exécution d'un sous-programme, un code (CIP2) d'identification du programme ayant appelé le sous-programme.

5. Microprocesseur selon la revendication 4, caractérisé en ce que le système d'attribution de droits comprend des moyens pour appliquer simultanément sur la première entrée (E1) de la table d'attribution de droits, pendant l'exécution d'un sous-programme, un code (CIP1) d'identification du sous-programme en cours d'exécution et un code (CIP2) d'identification du programme ayant appelé le sous programme.

6. Microprocesseur selon la revendication 5, caractérisé en ce que ce que des bits (b0', b1') du code (CIP2) d'identification du sous-programme en cours d'exécution et des bits (b0", b1") du code d'identification du programme ayant appelé le sous programme sont combinés par une fonction logique (11) avant d'être appliqués sur la première entrée (E1) de la table d'attribution de droits (TDA, TDA1, TDA3).

7. Microprocesseur selon l'une des revendications 4 à 6, caractérisé en ce que le système d'attribution de droits comprend :

- un premier verrou (LT1) pour stocker (LOAD1) pendant l'exécution d'une instruction le code (CIP1) d'identification du programme ou du sous-programme en cours d'exécution,
- un second verrou (LT2) ayant son entrée reliée à la sortie du premier verrou, agencé pour stocker (LOAD2) le code (CIP1) d'identification d'un programme en cours d'exécution lorsque le microprocesseur bascule dans un sous-programme, pour former le code (CIP2) d'identification du programme ayant appelé le sous-

programme, le second verrou étant remis à zéro (RST) lorsque le microprocesseur quitte le sous-programme.

8. Microprocesseur selon la revendication 7, caractérisé en ce que le chargement et la remise à zéro du deuxième verrou (LT2) sont contrôlés par un décodeur d'adresse (DEC2) recevant en entrée les adresses courantes (ADR) circulant sur le bus d'adresse, agencé pour appliquer un signal de chargement (LOAD2) au second verrou lorsque l'adresse (ADRin) de la première instruction d'un sous-programme est détectée, et délivrer au second verrou un signal de remise à zéro (RST) lorsque l'adresse (ADRout) de la dernière instruction du sous-programme est détectée.

9. Microprocesseur selon l'une des revendications 4 à 8, caractérisé en ce que les codes (CIM) d'identification des zones mémoire désignées par les adresses courantes et les codes (CIP1) d'identification des programmes et sous-programmes en cours d'exécution sont délivrés par un décodeur d'adresse (DEC1) recevant en entrée les adresses courantes circulant sur le bus d'adresse.

10. Microprocesseur selon l'une des revendications 1 à 8, caractérisé en ce que le système d'attribution de droits (10) émet un signal de violation (VLT) quand une adresse présente sur le bus d'adresse ne correspond pas aux droits attribués de façon permanente ou temporaire au programme ou sous-programme en cours d'exécution.

11. Microprocesseur selon la revendication 10, caractérisé en ce que le signal de violation d'adresse (VLT) est traité par un décodeur d'interruption (ITDEC) pour envoyer le microprocesseur dans un sous-programme (ITADR) de traitement des violations d'adresse.

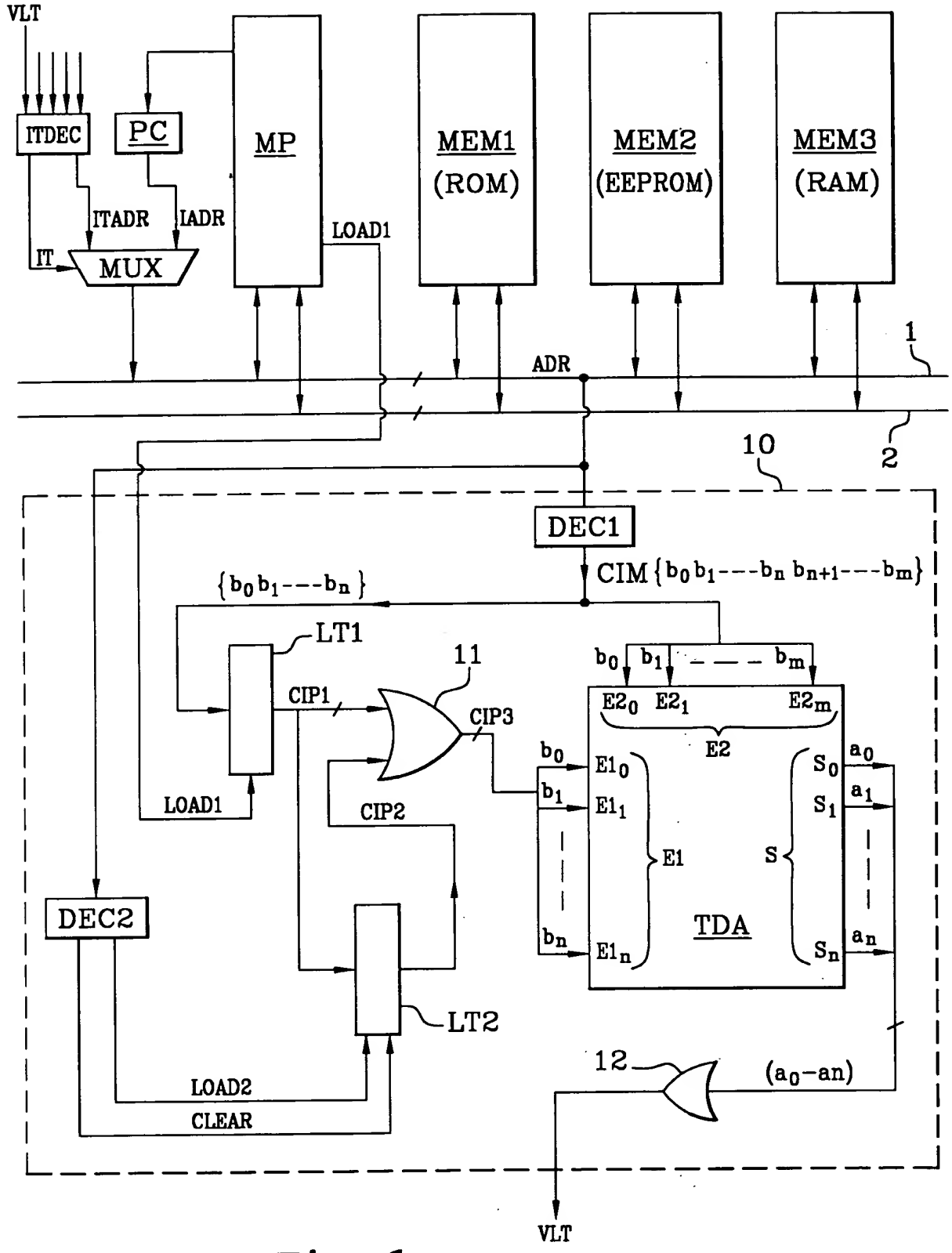
VLT
ITDEC
PC
MP
MEM1
(ROM)
MEM2
(EEPROM)
MEM3
(RAM)
ITADR
IADR
IT
MUX
LOAD1
ADR
1
2
10
DEC1
CIM {b0 b1---bn bn+1---bm}
{b0 b1---bn}
LT1
11
CIP1
CIP3
CIP2
LOAD1
b0 b1 ---- bm
E20 E21 E2m
E2
b0
b1
bn
E10
E11
E1n
E1
S
S0
S1
Sn
a0
a1
an
TDA
DEC2
LT2
12
(a0-an)
LOAD2
CLEAR
VLT

Fig. 1

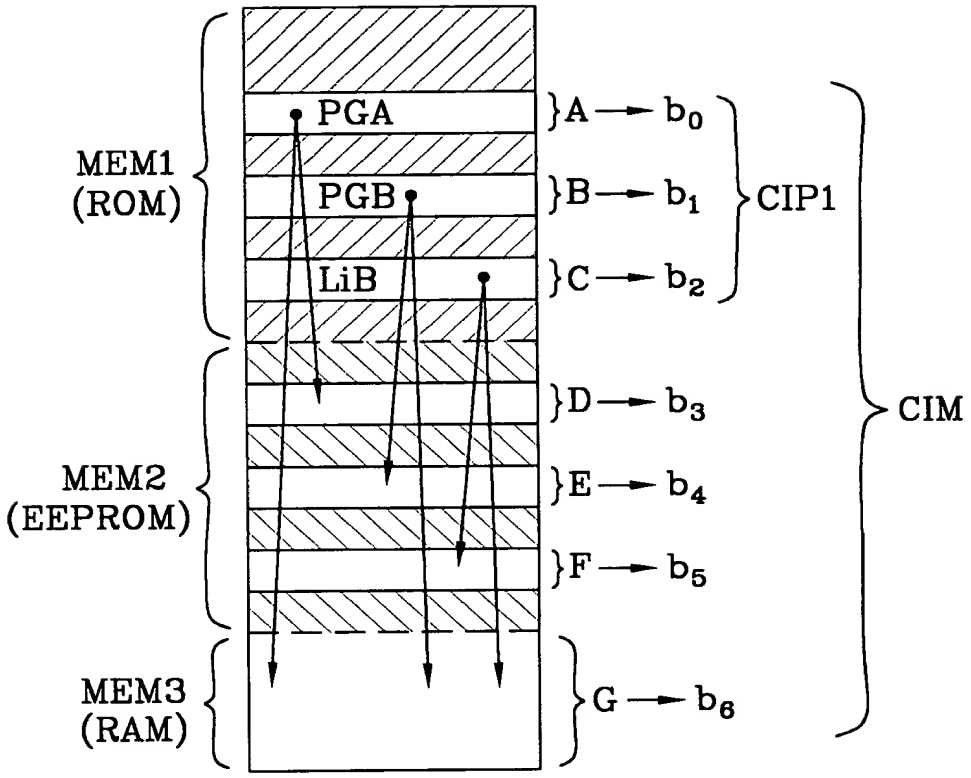
MEM1
(ROM)
MEM2
(EEPROM)
MEM3
(RAM)
PGA
PGB
LiB
}A → b0
}B → b1
}C → b2
}D → b3
}E → b4
}F → b5
}G → b6
CIP1
CIM

Fig. 2

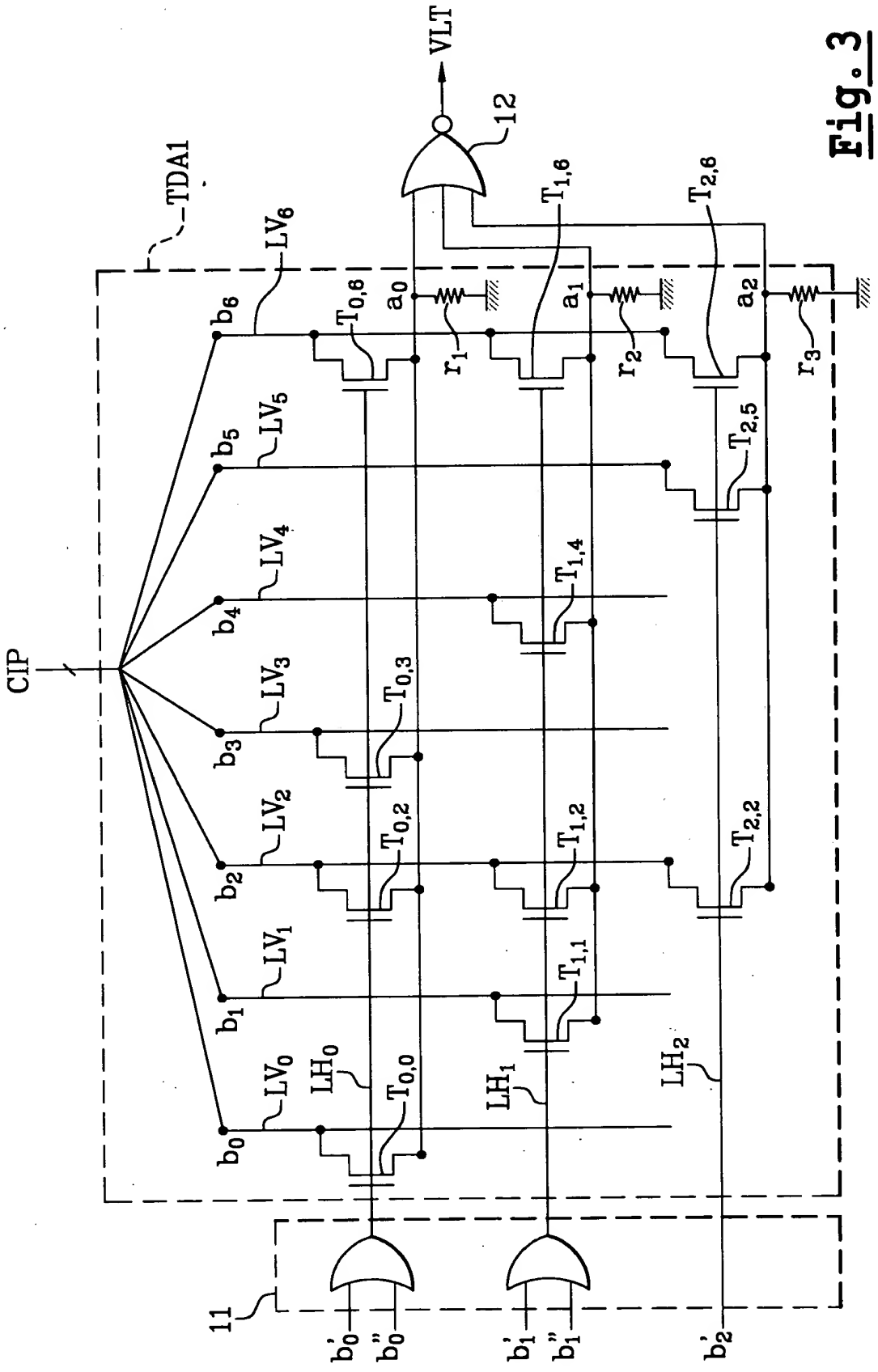
VLT
12
TDA1
LV6
LV5
LV4
LV3
LV2
LV1
LV0
CIP
b6
b5
b4
b3
b2
b1
b0
a0
a1
a2
r1
r2
r3
T0,6
T0,3
T0,2
T0,0
T1,6
T1,4
T1,2
T1,1
T2,6
T2,5
T2,2
LH0
LH1
LH2
11
b'0
b"0
b'1
b"1
b'2

Fig. 3

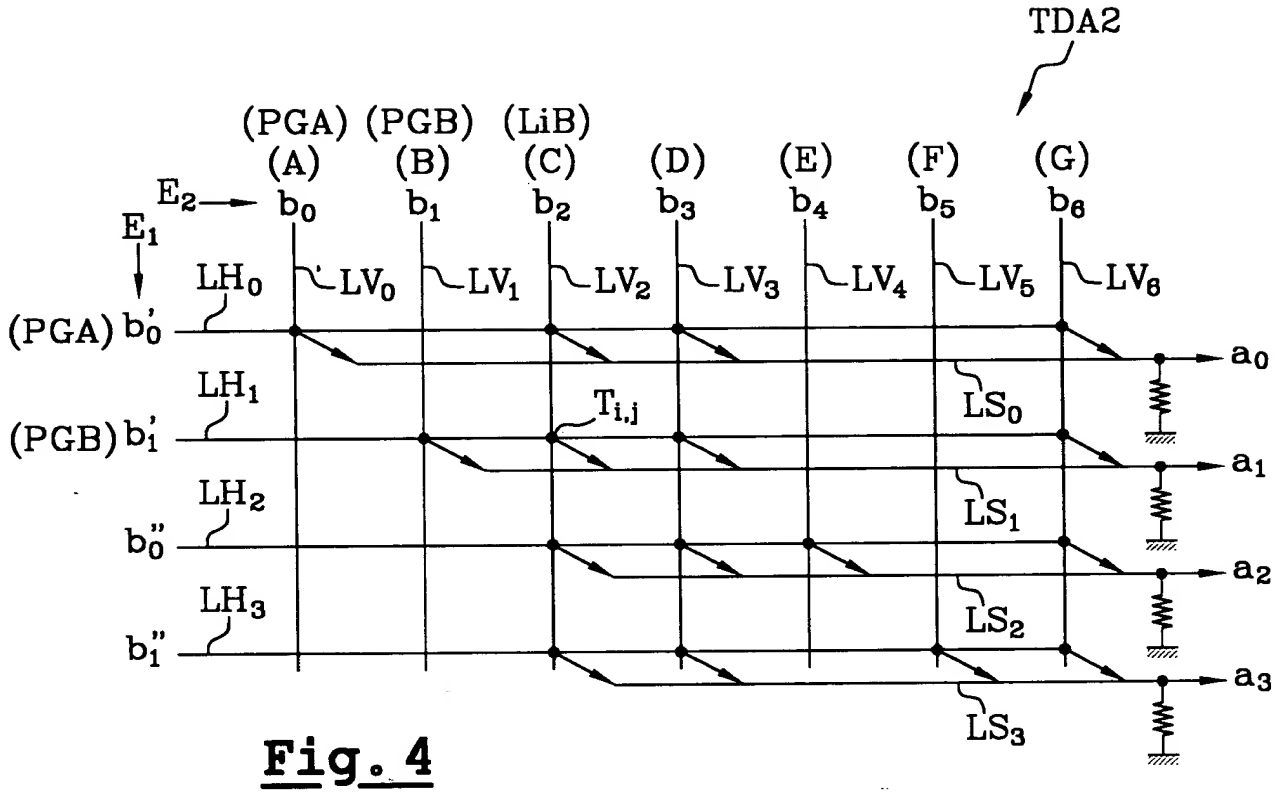
TDA2
(PGA) (PGB) (LiB)
(A) (B) (C) (D) (E) (F) (G)
E2
E1
b0 b1 b2 b3 b4 b5 b6
LH0
LV0 LV1 LV2 LV3 LV4 LV5 LV6
(PGA) b'0
LH1
(PGB) b'1
Ti,j
LS0
a0
a1
LH2
b''0
LS1
a2
LH3
b''1
LS2
a3
LS3

Fig. 4

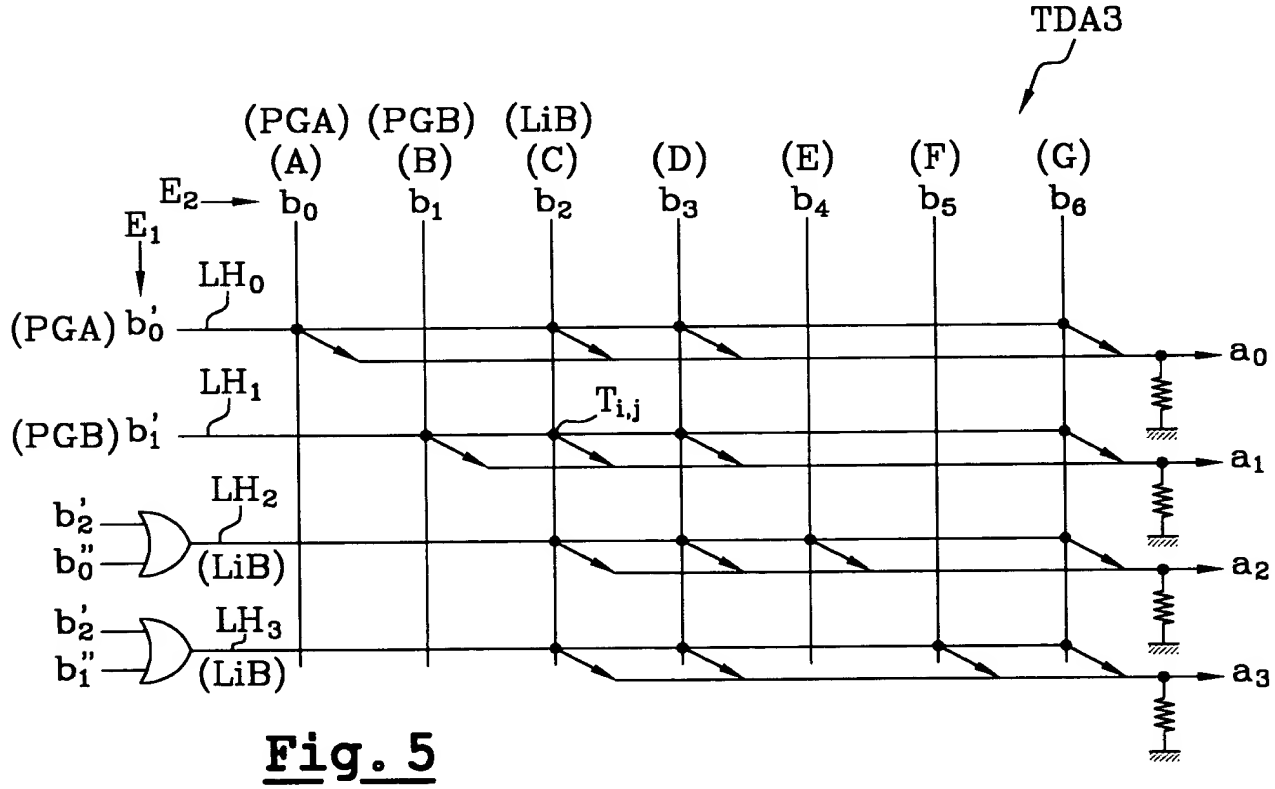
TDA3
(PGA) (PGB) (LiB)
(A) (B) (C) (D) (E) (F) (G)
E2
E1
b0 b1 b2 b3 b4 b5 b6
LH0
(PGA) b'0
LH1
(PGB) b'1
Ti,j
a0
a1
b'2
LH2
b''0
(LiB)
a2
b'2
LH3
b''1
(LiB)
a3

Fig. 5